Docket No. AT9-98-737   *PATENT*
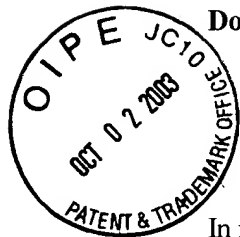
#18
LBJ
10-21-03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
OCT 0 8 2003
Technology Center 2100

In re application of: **Chavez, Jr.**

Serial No.: **09/292,190**   Group Art Unit: **2155**

Filed: **April 15, 1999**   Examiner: **Dinh, Khanh Q.**

For: **Method and System for Enabling a
Network Function in a Context of One or All
Server Names in a Multiple Server Name
Environment**

**Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450**

**ATTENTION: Board of Patent Appeals
and Interferences**

<table>
<tr><td>

</td></tr>
</table>

APPELLANT'S BRIEF (37 C.F.R. 1.192)

This brief is in furtherance of the Notice of Appeal, filed in this case on August 5,

2003.

The fees required under § 1.17(c), and any required petition for extension of time for

filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF

APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. 1.192(a))

10/06/2003 SDENBOB1 00000110 090447   09292190

01 FC:1402   320.00 DA

REAL PARTIES IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines, Inc.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-22

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-22
4. Claims allowed: 8-11 and 18-20[1]
5. Claims objected to: NONE
6. Claims rejected: 1-7, 12-17, 21 and 22

C. CLAIMS ON APPEAL

The claims on appeal are: 1-7, 12-17, 21 and 22.

---

[1] It should be noted that the Office Action Summary sheet of the Final Office Action indicates these claims to be objected to. However, the body of the rejection correctly indicates these claims to be allowed.

STATUS OF AMENDMENTS

No amendments have been filed after issuance of the Final Office Action. A Response to the Final Office Action was filed on June 5, 2003 containing only remarks.

SUMMARY OF INVENTION

The present invention provides a method of executing a function on a server in a distributed data processing system. The server responds to requests directed to a set of server names. A function request has an input that specifies a server name in the set of server names. The function is executed on the server in a server name context specified by the input containing the server name. The server name context on the server has a set of resources associated with a server name. A unique server name tag is generated for each server name in the set of server names and each resource in the set of resources is identifiable by the server name tag associatively stored with the resource. In a preferred embodiment, a server name mask is generated based on the server name specified in the function request and the function is executed in a server name context on a server based on the generated server name mask.

ISSUES

The only issue on appeal is whether claims 1-7, 12-17, 21 and 22 are obvious under 35 U.S.C. § 103(a) in view of French et al. (U.S. Patent No. 6,442,685) and Nishimoto et al. (U.S. Patent No. 6,199,164).

GROUPING OF CLAIMS

The claims do not stand or fall together. The grouping of claims is as follows:

Group I – claims 1-4, 7, 12-15, 21 and 22;

Group II – claims 5 and 16; and

Group III –claims 6 and 17.

ARGUMENT

I.   35 U.S.C. § 103, Alleged Obviousness

The Office Action rejects claims 1-7, 12-17 and 21-22 under 35 U.S.C. § 103(a) as being unpatentable over French et al. (U.S. Patent No. 6,442,685) in view of Nishimoto et al. (U.S. Patent No. 6,199,164). This rejection is respectfully traversed.

A.   Group I – Claims 1, 12 and 21

French discloses a method and system that allows for multiple network names on a single server. With the method and system of French, a primary server name and one or more secondary server names are registered with a server via a configuration file. The server is able to respond to requests directed to either the primary server name or the one or more secondary server names. In this way, when a server fails, another server in the cluster may take over responding to requests to that server name.

Claim 1, which is representative of the other rejected independent claims 12 and 21 with regard to similarly recited subject matter, reads as follows:

> 1.   A method for executing a function on a server in a distributed data processing system, the method comprising the computer-implemented steps of:
>   receiving a request for a function, wherein the request comprises an input specifying a server name, wherein the server responds to requests directed to a set of server names;
>   generating a server name mask based on the server name; and
>   executing the function in a server name context on the server, as directed by the input specifying the server name, based on the generated server name mask. (emphasis added)

French does not teach the generation of a server name mask or the execution of a function in a server name context based on a generated server name mask. While French teaches that a configuration file for a server may have a primary server name and a plurality of secondary server names to which a server responds, there is no teaching in French to generate a server name mask based on a server name specified in a request for a function.

In fact, there is no mention whatsoever in French regarding masks, let alone a server name mask. The Office Action is in agreement and admits that French "does not specifically disclose using a server name mask based on a server name" (Office Action, page 1, section 3).

However, the Office Action alleges that this feature is taught by Nishimoto in Figures 7, 20A and 20B, the abstract, column 12, line 20 to column 13, line 60, and column 23, line 1 to column 24, line 60. Appellant respectfully disagrees.

Nishimoto is directed to an information management system and apparatus using an open network environment. The system of Nishimoto is directed to solving the problems of freshness of information being dependent on the frequency with which a user accesses a server and the user having to input personal information every time they access a different service (see column 1, lines 44-66, for example). In order to solve these problems, Nishimoto allows a user to register with a connection server information regarding the types of information that the user is interested in and the priority of the communication channels, e.g., emergency, regular confirmation, and preservation channels, that IP servers may use to send information to the user's client device.

That is, the user of a client device registers public personal information (see Figure 8) and connection permission information (see Figure 5) with a connection server. The public personal information includes the information regarding an ID of the user, the kinds of information that are necessary, e.g., real estate exchange, stock exchange, conference schedule, etc. (see column 12, lines 44-67), and personal information including name, address, telephone number, etc. The connection permission information includes a designation for each channel type, those IP servers that are allowed to communicate with the client device over that type of channel and those IP servers that are not allowed to communicate with the client device over that type of channel. This may include a list of a plurality of names of IP servers.

The details of how the system works are set forth in column 18, line 35 to column 21, line 47. In this section of Nishimoto, the operation of the system is described as the user editing their public information 102 to input "real estate" into the kind of necessary information of the inevitable public items 148, the ID code of the user A is already allocated and is used to automatically form connection information having the ID code "xyz." The

connection information is transmitted to the connect server 12 which registers the connection information. The client device 10 then sends the public personal information to the connection server 12 which updates and registers a record of the public personal information. When the public personal information is registered, the connection server 12 recognizes that "real estate" is a kind of necessary information and transmits a registration form for special personal information registration which has been specialized for "real estate" to the client device 10. The user may then edit this form to input the information which is of interest to the user (see the example in column 21, lines 14-17).

Periodically, the IP server 14 of a real estate company request connection server 12 to retrieve the ID code having an access permission that allows the real estate company to access the public personal information associated with the ID code. The connection server 12 transmits the registered ID codes for which access permission is allowed. As a result, the ID code "xyz" is transmitted to the IP server 14. The IP server 14 then requests the public personal information for the ID code. The connection server 12 then returns the public personal information to the IP server 14, which includes the designation of "real estate" as necessary information.

The IP server 14 then, having determined that the ID code "xyz" has a necessary information type of "real estate", requests the connection information for this ID code. The connection server 14 refers to the connection permission information associated with the ID code "xyz" and recognizes that the permission IP server host name "All" is associated with the preservation channel. As a result, a masking operation is performed so as to remove the password for the emergency channel and regular confirmation channel and leave only the password of the permitted preservation channel (see column 20, lines 45-51). The IP address and preservation channel password in which the reception of information is permitted are then provided to the IP server 14. The IP server 14 may then request that the client 10 permit transmission using the preservation channel.

Nishimoto does not teach or suggest generating a server name mask based on a server name or executing a function in a server name context on a server based on the generated server name mask, as recited in independent claim 1. The "mask" referenced in Figure 16A step S108, 17E, 18B step S105, 19D, 24A step S108, 25A step S111, and 33 step S3, is the masking of passwords associated with the various channels, i.e.

emergency, regular confirmation, and preservation channels (see column 20, lines 43-51; column 22, lines 10-34; column 23, lines 58-67; column 24, lines 20-23 and 46-48; and column 25, lines 54-60). That is, "masking" in the context of Nishimoto involves only sending connection information, i.e. the IP address of the client and the password, associated with a connection type with which the server may communicate with the client. Thus, for example, if the server is only allowed to communicate with the client via an emergency channel, then only the IP address and password associated with the emergency channel is sent to the server (see column 25, lines 54-60, for example).

The "masking" of Nishimoto is not associated with the generation of a server name mask based on a server name and is not used to execute a function in a server name context on a server. To the contrary, the "masking" in Nishimoto is used to send the IP address and password to the server for only the channels that the server can use to communicate with the client as defined by the connection permissions. The "mask" of Nishimoto has nothing to do with executing a function in a server name context and is not generated based on a server name. Thus, since the Office Action admits that French does not teach this feature, and Nishimoto has been shown to not teach or suggest this feature either, any alleged combination of Nishimoto and French cannot be found to teach this feature.

In addition, it is clear from the above explanation of the Nishimoto reference, that Nishimoto is directed to a completely different system than that of either the French reference or the present invention. The Nishimoto reference is directed to a system for allowing servers to initiate information downloads to client devices based on registered information types of interest to the users of the client devices and their designated channel permissions. French is directed to a method and system for allowing a single server to respond to multiple network names. These two systems are completely different and one of ordinary skill in the art would not have found it obvious to combine them in the manner alleged by the Office Action. Furthermore, it is not at all clear how one of ordinary skill in the art would combine these references assuming he/she were somehow motivated to do so.

Moreover, the alleged motivation provided by the Office Action is not based on the actual teachings of the references and is erroneous. The Office Action alleges that the

motivation to combine Nishimoto with French is "because it would have provided a masking process to the personal information and provided a more secure network environment." The masking in Nishimoto is not performed on personal information. To the contrary, the masking in Nishimoto is directed to connection information, namely the IP address and password used by the server to transmit information to the client over a particular priority communication channel, i.e. emergency, regular confirmation, or preservation. Moreover, the masking is not performed to increase the security of the system but is rather used as a way for the user of the client device to control which IP servers may send information to the client and at which priorities the information is to be displayed on the client. Thus, the alleged motivation is not based in the actual teachings of the references and is rather an erroneous allegation used to bolster an attempted hindsight reconstruction of Appellant's claimed invention having first had benefit of Appellant's disclosure.

Thus, in view of the above, Appellant respectfully submits that neither French nor Nishimoto, either alone or in combination, teaches or suggests the features of independent claims 1, 12 and 21. At least by virtue of their dependency on claims 1, 12 and 21, respectively, Appellant respectfully submits that neither French nor Nishimoto, either alone or in combination, teach or suggest the features of dependent claims 2-7, 13-17 and 22. Accordingly, Appellant respectfully requests withdrawal of the rejection of claims 1-7, 12-17 and 21-22 under 35 U.S.C. § 103(a).

B.   Examiner's Response to Arguments

In the Advisory Action mailed June 26, 2003, the Examiner responds to the above arguments with the following:

> Examiner respectfully disagrees. Nishimoto clearly discloses the masking process based on the retrieval of host server names by using retrieval to the connection information retrieval responding (including ID code) unit of the connection server (see col. 12 line 20 to col. 13 line 60 and col. 23 line 1 to col. 224 line 60).
> In response to Applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only

be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have provided a masking process to the personal information and provided a more secure network environment.

The portions of Nishimoto that the Examiner alleges support the Examiner's allegations of obviousness are reproduced below. Column 12, line 20 to column 13, line 60 reads as follows:

FIG. 7 shows the connection notification destination information 100 which is stored into the connecting situation database 36 provided for the connection server 12 in FIGS. 2A to 2C. The ID code 124 of the peer client 10 which registered and a host name 146 of the IP server serving as a connection notification destination are stored in the connection notification destination information 100. That is, the connection notification destination information registration format 60 is read out and the connection notification destination information 100 is edited by the public personal information processing unit 54 of the peer client 10 in FIGS. 2A to 2C and is transmitted together with the connection information and the like when the connection to the connection server 12 is started and is registered into the connecting situation database 36. The connection notification destination information 100 is referred to when the peer client 10 is connected to the network and the connection information is preferentially notified from the connection server to the IP server registered as a notification destination without retrieving. Thus, an advantage such that the connection information is transmitted to the IP server which is frequently used simultaneously with the connection of the peer client to the network and, if there is providing information, it can be immediately received can be derived.

FIG. 8 shows the public personal information 102 which is registered into the public personal information database 38 provided for the connection server 12 in FIGS. 2A to 2C. In the public personal information 102, inevitable public items 148 and option public items 150 are provided subsequent to the ID code of the peer client 10. The inevitable public items 148 are information which is fixedly opened. A kind 152 of necessary information and a kind 154 of unnecessary information to the IP server 14 can be registered in the inevitable public items 148. The option public items 150 are items in which the opening and the non-opening can be selectively designated by the public personal information use permission information 104 in FIG. 9 and it is also

possible to register nothing about it on the basis of a judgment of the user. In the example, the option public items 150 include a name 156, an address 158, a telephone number 160, a facsimile FAX 162, a mail address 166, and others 168. If the user of the peer client 10 wants to make an access permission to obtain information which the user desires to receive for the first time to the connection server 12, all of the option public items 150 are not opened and information and kinds of services such as "real estate exchange", "stock exchange", "exchange trading", "conference schedule", and the like which the user wants to be provided are registered in the kind 152 of necessary information in the inevitable public items 148. As for the kind 154 of unnecessary information in the inevitable public items 148, the kind 152 of necessary information is once set and registered into the public personal information database 38 of the connection server 12. After that, if the user wants to stop the providing of the registered services, the registered items are deleted from the kind 152 of necessary information. However, when the stop of the providing cannot be protected due to some errors, in order to clearly stop, it is sufficient to register the kind of unnecessary information to be stopped. As will be obviously understood from the public personal information 102, in the information management system of the invention, the public personal information which is first provided to the connection server 12 is only the ID code 124 of the peer client 10 and the kind 152 of necessary information set in the inevitable public items 148. It is possible to receive initial approaches from the IP servers 14 of a plurality of information providers corresponding to the kind of necessary information which are connected to the internet by the necessary least public personal information.

The public personal information use permission information 104 in FIG. 9 is constructed by inevitable public item use permission information 170, option public item use permission information 172, an active publication 174, and the ID code 124. In the inevitable public item use permission information 170, a permission IP server host name and a refusal IP server host name are registered, a default of the permission IP server host name is set to "All", and a default of the refusal IP server host name is set to "none" in correspondence to "All". Likewise, with respect to the option public item use permission information 172 as well, a permission IP server host name and a refusal IP server host name can be registered. A default of the permission IP server host name is set to "none" and a default of the refusal IP server host name is set to "All". Therefore, in the default state, the inevitable public items 148 of the public personal information 102 in FIG. 8 are set to "use permission" and the option public items 150 are set to "use refusal". In the active publication 174 in the public personal information use permission information 104, the presence or absence of the active publication is set. A default value is set such that the active publication is "not done". By setting the active publication 174 to "done", when the peer client 10 sends the connection information and

the public personal information to the connection server at the start of the connection to the network and registers them into the database, the public personal information is actively provided to the IP server. That is, when it is recognized that the active publication 174 has been set to "done" in the public personal information use permission information 104, the connection server 12 refers to the kind of necessary information and the kind of unnecessary information registered in the inevitable public items 148. A kind 190 of providing information of the data of the information provider in FIG. 11 obtains a relevant IP server host name 192. The connection server 12 actively transmits information indicating that an access permission and an access refusal have already been issued to a plurality of IP servers 14 having those IP server host names, thereby realizing a more rapid and efficient information providing from the IP server 14 side.

It should first be noted that the word "mask" does not appear anywhere in this section of Nishimoto. Therefore, it is not clear how a section of a reference that does not even mention the term "mask" can be found to teach or suggest a server name mask or executing a function in a server name context based on a server name mask. Moreover, this section of Nishimoto merely teaches that the connection notification destination information includes an ID code of a peer client and a host name of an IP server serving as a connection notification destination. This information is transmitted together with connection information to the connection server.

In addition, this section of Nishimoto further teaches that public personal information may include inevitable public items and option public items. The option public items may include the designation of the kinds of information the user wishes to receive, e.g., "real estate exchange", "stock exchange", etc. The information that is provided to the connection server is only the ID code for the peer client and the kinds of information that the user wishes to receive.

Furthermore, this section of Nishimoto teaches that public personal information use permission information includes a permission IP server host name and a refusal IP server host name, along with default server host names. In a default state, the inevitable public items of the public personal information are set to "use permission" and the option public items are set to "use refusal."

There is nothing in this section of Nishimoto that teaches or even suggests the generation of a server name mask or the execution of a function in a server name context

based on a server name mask. While this section may teach registering IDs of peer computers, a connection server host name, types of information desired, etc. there is not so much as a hint at server name masks, server name contexts, a function being executed in a server name context, let alone a function being executed in a server name context based on a generated server name mask.

Column 23, line 1 to column 24, line 60 reads as follows:

Referring again to FIGS. 20A and 20B, after completion of the edition of the public personal information use permission information in step S2, the public personal information is edited in step S3. For example, as shown in the public personal information 102 of the connection server 12 in FIGS. 22A to 22C, since the option public items 150 are opened by the edition of the public personal information use permission information 104, the user A inputs "aa@bb. cc. dd" as a self mail address 166 into the option public items 150 and inputs "A" into the name 156. Therefore, by obtaining the option public items 150 of the edited public personal information 102, the real estate company I of an IP server 14-1 can recognize for the first time that the user is A. Subsequently in step S4 in FIGS. 20A and 20B, the connection permission information is edited. In this case, the emergency channel is permitted to only the real estate company I and, with respect to the regular confirmation channel and the preservation channel, the real estate company J is refused. That is, as shown in the connection permission information 96 of the connection server 12 in FIGS. 22A to 22C, "I company" is set into a permission IP server host name 218 of the emergency channel 138 and "J company" is inputted to refusal IP server host names 220 and 222 of the regular confirmation channel 140 and preservation channel 142, respectively. Subsequently in step S5 in FIGS. 20A and 20B, when connecting to the internet 16 after the next time by the edition of the connection notification destination information, the operation is designated so as to notify of a fact that the connection to the real estate company I was performed. That is, as shown in the connection notification destination information 100 of the connection server 12 in FIGS. 22A to 22C, "I company, IP server host name" is set as an IP server host name 146 of the connection notification destination. After completion of the edition of each information in steps S2 to S5 as mentioned above, the connection to the internet 16 is started in step S6. The transmission by the automatic formation of the connection information and the transmission of each of the information which has already been edited are executed for the connection server 12 in step S7. Each information is updated and registered into the database in step S101. In this instance, as shown in the public personal information use permission information 104 of the connection server 12 in FIGS. 22A to 22C, since the active publication 174 has been set to "done" with respect

to the ID code "xyz" of the user A, the active publication is recognized. In step S102, a fact that there is a change in database registration information in the connection server 12 is notified to a plurality of IP servers 14 of the real estate company group. In the plurality of IP servers 14 of the real estate company group which received the change notification based on the active publication, if the special personal information of the ID code "xyz" of the user A has been registered in the special personal information database, it is deleted. The public personal information 102 like an I company IP server 14-1 in FIGS. 22A to 22C is obtained, so that it is possible to know that the user of the ID code "xyz" is Mr. A and to know his mail address. When the information which the real estate company I wants to transmit is generated in step S202 in FIGS. 20A and 20B, the retrieval of the connection information is requested to the connection server 12 by the retrieval ID in step S203 in FIG. 21. Thus, the connection information of the user A is transmitted via the masking process based on the retrieval acceptance, reference to the connection destination information, and reference to the connection permission information in step S103. The IP server 14 obtains the connection information in step S204. As for the connection information of the user A obtained by the real estate company I, the passwords have been opened with respect to all of the emergency channel, regular confirmation channel, and preservation channel as shown in the connection information 94-1 of the IP server 14-1 of the I company in FIGS. 22A to 22C. The IP server 14-1 of the real estate company I can transmit the information using the channel which is thought to be necessary.

On the other hand, when information which the other real estate company J wants to transmit is generated in step S301 in FIG. 21 accidentally or by a mistake although such a case ordinarily doesn't occur because the ID code "xyz" has been deleted from the special personal information database or has been inactivated, the connection server 12 is requested to retrieve the connection information by using "xyz" of the user A in step S302. In response to the retrieval request, the connection server 12 similarly executes an acceptance of the retrieval, a reference to the connection destination information, and a reference to the connection permission information, executes the masking process to the connection information, and after that, transmits the resultant information in step S104. An IP server 14-2 of the real estate company J gets the connection information in step S303. The contents of the connection information are "absent on net" as shown in the connection information 94-2 of the IP server 14-2 of J company in FIGS. 22A to 22C. That is, as for the public personal information 102 registered in the connection server 12, the kind 154 of unnecessary information of the inevitable public items 148 has been set to "real estate". Therefore, in the public personal information 102-2 which is obtained by the IP server 14-2 of the J company, the kind of necessary information has been set to "none". Thus, the ID code "xyz" of the user A is eventually excluded from the access targets of the J company

IP server 14-2 which provides the information regarding the real estate. At a time point when it is recognized, it is desirable to delete the record of the ID code "xyz" from the special personal information database 48. For a retrieval request of the connection information in which the ID code "xyz" was designated from the IP server 14-2 of the J company due to an accidental purpose or a mistake which ordinarily cannot occur, in the connection permission information 96 of the connection server 12, the real estate company J has been registered to "refusal IP server host name" with respect to all of the emergency channel 138, regular confirmation channel 140, and preservation channel 142, so that the passwords of all of the channels in the original connection information 94-1 are mask-processed. In the J company IP server 14-2, thus, only "absent on net" like connection information 94-2 can be accepted as a response of the retrieval request by the ID code "xyz", so that the transmission of the information to the user A is refused. It is desired that, at a time point when the above process is continuously performed a few times, the record of the ID code "xyz" of the user A is deleted from the special personal information database 48.

§2 Adjustment of conference schedule.

FIGS. 23A, 23B, 24A, 24B, 25A, and 25B show the details of the system operation when a conference schedule is adjusted by the information management system of the invention in FIGS. 1A and 1B.

The only statement in the above cited portion of Nishimoto that makes any reference to a mask of any sort is the statement "Thus, the connection information of the user A is transmitted via the masking process based on the retrieval acceptance, reference to the connection destination information, and reference to the connection permission information in step S103." The "masking" process referenced here, as discussed above, is with regard to the sending of the IP address and password to the server for only the channels that the server can use to communicate with the client as defined by the connection permissions. The "mask" of Nishimoto has nothing to do with a server name mask generated based on a server name included in a function request nor does it provide any teaching regarding executing a function in a server name context and is not generated based on a server name.

Thus, the sections of Nishimoto that the Examiner alleges supports the finding of obviousness, as illustrated above, in actuality does not provide any teaching or suggestion regarding a server name mask generated based on a server name designated in a function request nor do they provide any teaching or suggestion regarding executing a function in a

server name context based on such a server name mask.

Furthermore, with regard to the Examiner's statements in response to Appellant's assertion of hindsight reconstruction, Appellants recognize that all examination includes some measure of hindsight. However, if the rejection of the claims is completely based on hindsight, as in the present case, then the rejection is improper. That is, while the Examiner must be aware of the present invention in order to search for prior art, once the prior art is found, the Examiner must view the art from a standpoint that does not include the teachings obtained from Appellant's disclosure. The Examiner must answer the question, if one of ordinary skill in the art were presented with French and Nishimoto alone, and without having known about Appellant's claimed invention, would one of ordinary skill in the art be motivated to combine and/or modify the features of the references in the specific manner necessary to arrive at the claimed invention? Appellants respectfully submit that in the present case, the answer to this question is no.

If one of ordinary skill in the art were presented only with French and Nishimoto, there is no teaching or suggestion that would lead that person of ordinary skill in the art to combine and/or modify the teachings of the references in the specific manner necessary to arrive at Appellant's claimed invention. In the present case, the first reference is French which is directed to a mechanism for allowing a server to respond to a primary server name and a plurality of secondary server names. The mechanism of French uses a configuration file that designates the primary and secondary server names and which is used to determine which traffic can be handled by that server. There is no statement in French that there is any deficiency in this approach for which the generation of a server name mask and the execution of a function in a server name context based on a generated server name mask would be a solution.

The second reference is Nishimoto, which is directed to a mechanism for designating what information a peer computing device is to receive from various information providers. While Nishimoto teaches a mask, it has nothing to do with designating what names a server responds to, is not generated based on a server name designated in a function request, and is not used as a basis for executing a function in a server name context. Moreover, there is no teaching or suggestion in Nishimoto that the masking process in Nishimoto could be used to execute functions in a server name

context based on a server name mask generated based on a server name included in a function request.

There simply is no teaching or suggestion in either reference to make the alleged combination or the modifications that would be necessary to arrive at the presently claimed invention as set forth in claims 1, 12 and 21. In other words, there is no teaching or suggestion in either reference to extract the teaching of a masking process from Nishimoto, modify the masking process so that it no longer identifies the types of information that a user is interested in receiving, and instead generates a server name mask based on a server name designated in a function request, and then modifying the French system to no longer use a server configuration file that identifies the primary and secondary server names to which a server responds, and instead use the server name mask to execute functions in a server name context based on the server name mask.

In fact, even if one were somehow motivated to attempt a combination of French and Nishimoto, which they would not be without having first had benefit of Appellant's claimed invention and the sole purpose of attempting to recreate Appellant's claimed invention, the result would not be the invention as recited in claims 1, 12 and 21. To the contrary, the combination would be some odd combination of a system in which a server may respond to various server names based on primary and secondary server names designated in a configuration file and a system in which the information sources that a user wishes to receive information from are identified based on a masking process during registration of the user's peer computer with a connection server. The result would not be a system in which a server name mask is generated based on a server name designated in a function request and a system in which a function is executed in a server name context based on such a server name mask.

Thus, in summary, the Examiner's alleged support for the rejection of claims 1-7, 12-17, 21 and 22 falls far short of demonstrating the alleged "obviousness" of Appellant's claimed invention. The alleged combination of French and Nishimoto does not obviate the claimed invention.

C. Group II – Claims 5 and 16

In addition to the above, neither French nor Nishimoto, either alone or in combination, teach or suggest the specific features recited in the dependent claims. For example, with regard to claims 5 and 16, French does not teach a server name tag that is generated based on a value of a server name and a value derived from a data structure that stores the server name. The Office Action alleges that this feature is taught in French at column 9, line 53 to column 10, line 54 and column 11 lines 3-67. Column 9, line 53 to column 10, line 54 discusses an exemplary failure of a server with another server assuming the responsibilities of the failed server, as depicted in Figures 9B-9D. As described, a server 904 is disconnected from the LAN 900 so that it can be reconfigured to assume the duties of the Inventory server. This reconfiguration may be manual through use of a command line interface by a system administrator. The system administrator may add the network name "Inventory" to the server names in a configuration file for the server 904 and server 904 may then be restarted. Upon restart, the server names in the configuration file are registered with the server name table of the network services administration module. Alternatively, these functions may be performed automatically.

Nowhere in columns 9 and 10 of French is it taught to generate a server name tag based on a value of a server name and a value derived from a data structure that stores the server name. All that is taught in French is the addition of a server name to a configuration file of a server that is to take over the responsibilities for a failed server and the registration of that server name in a server name table of a network services administration module.

Column 11, lines 3-67 of French teaches that the server 904, which is taking over the responsibilities for failed server 905, has access to the information previously stored by server 905 on a shared disk 906. In addition, the invention described in French may be used in a migration scenario in which a server that is initially configured to respond to multiple server names is reconfigured so that multiple servers may respond to those server names. Nowhere in column 11 is it taught to generate a server name tag based on a value of a server name and a value derived from a data structure that stores the server name.

Moreover, there is nothing in Nishimoto that teaches or suggests such a feature. Therefore, any alleged combination of French and Nishmoto still would not result in the features recited in claims 6 and 17. Thus, claims 6 and 17 are further distinguished over French and Nishimoto based on the specific features recited in these claims.

D.   Group III – Claims 6 and 17

With regard to claims 6 and 17, French does not teach that the value derived from the data structure is a position value of the server name within a server name table that stores the set of server names. The Office Action alleges that this feature is taught at column 7, line 12 to column 8, line 63 and column 9, line 53 to column 10, line 54 of French. The text of columns 9 and 10 has been addressed above with regard to claims 5 and 16. Nowhere in this text is it ever taught to generate a server name tag based on a value of a server name and a value from a data structure that is the position value of the server name within a server name table that stores the set of server names.

In addition, column 7, line 12 to column 8, line 63 of French teaches the software components within a server that provide for multiple network names on a server. These components include data structures 538 which contain server name table 542 that contains a set of server names, such as primary server name 543 and secondary server names 544-546. Only one primary name may be registered per server, but multiple secondary server names may be registered per server. At initialization, the server reads the configuration file and determines if parameters in the configuration file indicate a primary or secondary server name. If so, they are registered in the server name table of the network services administration module.

There is nothing in columns 7 or 8 that teaches or suggests to generate a server name tag based on a value of a server name and a value derived from a data structure that stores the server name, let alone the value being a position value of the server name within a server name table that stores the set of server names. There simply is nothing in French that teaches or suggests the features of claims 6 and 17.
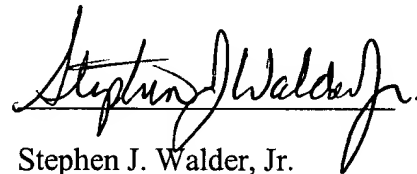
Moreover, there is nothing in Nishimoto that teaches or suggests such a feature. Therefore, any alleged combination of French and Nishmoto still would not result in the

features recited in claims 6 and 17. Thus, claims 6 and 17 are further distinguished over French and Nishimoto based on the specific features recited in these claims.

II.   CONCLUSION

In view of the above, Appellant respectfully submits that all of claims 1-22 are allowable over the cited prior art and that the application is in condition for allowance. Accordingly, Appellant respectfully requests the Board of Patent Appeals and Interferences to overturn the rejections set forth in the Final Office Action.

Respectfully submitted,

Stephen J. Walder, Jr.
Reg. No. 41,534
Carstens, Yee & Cahoon, LLP
PO Box 802334
Dallas, TX 75380
(972) 367-2001
Attorney for Appellant

APPENDIX OF CLAIMS

The text of the claims involved in the appeal are:

1.   A method for executing a function on a server in a distributed data processing system, the method comprising the computer-implemented steps of:

receiving a request for a function, wherein the request comprises an input specifying a server name, wherein the server responds to requests directed to a set of server names;

generating a server name mask based on the server name; and

executing the function in a server name context on the server, as directed by the input specifying the server name, based on the generated server name mask.

2.   The method of claim 1 wherein the server name context on the server comprises a set of resources associated with a server name.

3.   The method of claim 2 further comprising identifying a membership of a resource within the set of resources for the server name context.

4.   The method of claim 3 further comprising generating a server name tag for the server name, wherein the membership of the resource in the set of resources is identifiable by the server name tag associatively stored with the resource.

5.   The method of claim 4 wherein the server name tag is generated based on a value of the server name and a value derived from a data structure that stores the server name.

6.   The method of claim 5 wherein the value derived from the data structure is a position value of the server name within a server name table that stores the set of server names.

7.   The method of claim 1 wherein the request for the function is received from a network.

12.   A data processing system comprising:

       means for receiving a request for a function, wherein the request comprises an input specifying a server name, wherein the server responds to requests directed to a set of server names;

       means for generating a server name mask based on the server name; and

       means for executing the function in a server name context on the server, as specified by the input containing the server name, based on the generated server name mask.

13.   The data processing system of claim 12 wherein the server name context on the server comprises a set of resources associated with a server name.

14.   The data processing system of claim 13 further comprising identification means

for identifying a membership of a resource within the set of resources for the server name

context.

15.   The data processing system of claim 14 further comprising generation means for

generating a server name tag for the server name, wherein the membership of the resource

in the set of resources is identifiable by the server name tag associatively stored with the

resource.

16.   The data processing system of claim 15 wherein the server name tag is generated

based on a value of the server name and a value derived from a data structure that stores

the server name.

17.   The data processing system of claim 16 wherein the value derived from the data

structure is a position value of the server name within a server name table that stores the

set of server names.

21.   A computer program product on a computer readable medium for use in a data

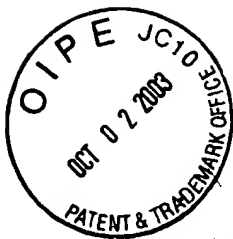processing system, the computer program product comprising:

        first instructions for receiving a request for a function, wherein the request

comprises an input specifying a server name, wherein the server responds to requests

directed to a set of server names;

        second instructions for generating a server name mask based on the server name

and

third instructions for executing the function in a server name context on the

server, as specified by the input containing the server name, based on the generated server

name mask.

22.   The computer program product of claim 21 wherein the server name context on

the server comprises a set of resources associated with a server name.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Chavez, Jr.**	§	Group Art Unit: **2155**
	§	
Serial No.: **09/292,190**	§	Examiner: **Dinh, Khanh Q.**
	§	
Filed: **April 15, 1999**	§	Attorney Docket No.: **AT9-98-737**
	§	

For: **Method and System for Enabling a Network Function in a Context of One or All Server Names in a Multiple Server Name Environment**

35525

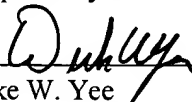PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appellant's Brief (in triplicate) (37 C.F.R. 1.192); and
- Our return postcard.

A fee of $320.00 is required for filing an Appellant's Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee
Duke W. Yee
Registration No. 34,285
CARSTENS, YEE & CAHOON, LLP
P.O. Box 802334
Dallas, Texas 75380
(972) 367-2001
ATTORNEY FOR APPLICANT